> the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization. Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information.[39]

Thus, the Committee Report makes clear that, while this provision includes the switch-based information equivalent to a seven or ten-digit phone number that directs a call when voice dialing or speed dialing features are used, it does not include location tracking information or any of the items contained in the FBI's punch list. While the Committee Report could not be clearer as to what Congress intended in this provision, the Act and its legislative history provide numerous additional clues indicating that the term cannot reasonably be read in the manner that the FBI urges.

1. The Express Language and the Legislative History of "Call-identifying Information" Mandate a Narrow Reading of the Provision

(a) CALEA does not mandate the capability to acquire "all" dialing and signaling information but only such information "that identifies the origin, direction, destination or termination" of a communication

Contrary to the FBI's repeated assertions that CALEA requires carriers to intercept "*all* communications and call-identifying information that law enforcement is authorized to acquire,"[40] Congress decided not to require carriers to deliver *all* call-identifying information. When the digital telephony bill (H.R. 4922/S. 2375) was introduced in August 1994, it defined call-identifying information as "*all* dialing or signaling information associated with the origin, direction, destination or termination of each communication." However, when the law was

---

[39] House Report at 21. As noted below, this is largely identical to (if anything slightly narrower than) the description used by the FBI for "call set-up information." Hearings at 277-78.

[40] FBI/DOJ Petition at 1. *See also* FBI/DOJ Petition at 2, 41.

enacted, the word "all" was dropped from the definition. This change shows that the call-identifying requirement does not cover all dialing or signaling information, but only a subcategory of that data – that which identifies the origin, direction, destination or termination of a communication.

The definition of call-identifying information only requires information "*that identifies* the origin, direction, destination or termination." The legislation, as introduced, used the broader phrase "dialing or signaling information *associated with* the origin, direction, destination or termination." However, as enacted, the phrase is more limited. Under CALEA, carriers need not implement network capabilities that can deliver *all* dialing or signaling information associated with the origin, direction, destination, or termination of a communication to law enforcement, but only the capability to deliver dialing or signaling information that identifies a communication's origin, direction, destination or termination.

Furthermore, the limitation beginning with the words "that identifies" applies to both "dialing" and "signaling." Even though "dialing" is a narrow word, Congress wanted to further limit it to exclude dialed number information that was not used for call processing. This was pursuant to the assurances of the FBI that it did not want to obtain with a pen register or trap and trace device the digits entered after call cut-through, and that it would treat as content any dialed number information transmitted after a communication had been established. As the Committees' report expressly states, "Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information."[41]

---

[41] House Report at 21.

(b) "Signaling" includes nothing beyond "dialing" information and therefore cannot be used to support location information or the punch list

Location information and many of the controversial elements of the FBI's punch list clearly do not fit within the meaning of the word "dialing." Therefore, the FBI's claim must rest solely on the word "signaling." But in this context, the word "signaling" must be read narrowly in conjunction with the word "dialing." Following the legislative history, "signaling" refers to the "messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carriers' network."[42]

It is a well-established rule of statutory construction that, when two words are grouped together in a statute, as these terms are in CALEA, and their meanings are disputed, the meaning of the broader or ambiguous word must be limited by the narrower or more precise term.[43] Accordingly, as the term "dialing" means the mere registering of numbers 0 through 9 on the telephone, and the transmission of those numbers over the line, "signaling" cannot be stretched to include other non-numerical information that the system may generate with or without customer action. The FBI's claim that the meaning of the term "signaling" is broader than that of the term "dialing" cannot be correct as it violates this fundamental concept of statutory interpretation.

This conclusion that "signaling" must be read narrowly in relation to "dialing" is further supported by the FBI's own testimony in connection with the legislation. Time and again, the FBI stated that it only wanted CALEA to preserve access to call content and "dialing

---

[42] *Id.*

[43] "If the legislative intent or meaning of a statute is not clear, the meaning of doubtful words may be determined by reference to their relationship with other associated words or phrases. Thus, when two or more words are grouped together, and ordinarily have a similar meaning, but are not equally comprehensive, the general word will be limited and qualified by the special word." Singer, Sutherland's Statutory Construction, § 47.16, 183

information."[44] And in response to a question about "transactional data," FBI Director Freeh assured Congress that the FBI was interested in dialed number information only:

I do not want that access [to transactional data], and I am willing to concede that. What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I have now under pen register authority.[45]

Moreover, in August 1994, when the legislation was introduced with the term "call-identifying information," the FBI Director testified again and praised the bill as a solution to law enforcement's need for "access to all communications and dialing information."[46]

Significantly, at no point during the legislative proceedings did the Director give any attention to the word "signaling," suggesting that, in his view, it was coextensive with the term "dialing." If the FBI had wanted Congress to treat the word "signaling" as something more, as it claims now, it should have brought such an interpretation to Congress' attention. Yet the FBI never did.

The word "signaling" was included in the statute in order to cover speed-dialing and voice-dialing -- services that allow a subscriber to initiate a call without dialing seven or ten digits. The problem posed by speed dialing is that a pen register on the customer line only picks

---

(5th ed. 1992) (footnotes omitted).

[44] When FBI Director Freeh appeared before a joint hearing of the House and Senate Judiciary subcommittees in March 1994, he said that the legislation would ensure "that the content of communications and call set-up information (dialing information) can be intercepted." Hearings at 27. Furthermore, in his prepared testimony on March 18, 1994, Freeh stated at least ten times that the legislation encompassed "communications and dialing information." *Id.* at 24 (two references to "dialing information"); 27 (four references); 28 (four references). Later, when the FBI submitted a list of the problems that justified enactment of CALEA, the second most frequent problem (after cellular port capacity) was the "[i]nability to capture dialed digits contemporaneous with audio." The third most common was "speed dialing/ voice dialing/ call waiting," where the problem was the unavailability of information identifying the phone number to which a call was being made. *Id.* at 121.

[45] *Id.* at 50.

up the memorized code for a particular phone number (e.g., the digit "1"), while the switch stores the seven or ten digit number that the customer's code signifies. Thus, for example, the customer "dials" a "1;" the switch produces a "signal" that corresponds to the 7 or 10 digit number needed to process the call. Through several references in the hearings, the FBI made clear that it needed a contemporaneous translation of the speed-dialing or voice-dialing commands into the seven or ten digit number; this is undoubtedly one of the problems the legislation was intended to address. The coupling together of the words "dialing or signaling" suggests that Congress intended to cover signaling information that is similar to dialing information; it offers no indication of an intent to include signaling information beyond that which is analogous to dialing information.

Finally, a broad reading of the term "signaling information" is inconsistent with Congress' apparent desire to respond to the fact that, for reasons unrelated to law enforcement's needs, the "signaling" channel was growing richer and richer as a source of personal information. There was great concern on the part of privacy advocates at the time CALEA was being debated that the signaling channel would be exploited by law enforcement based on the minimal pen register/trap and trace standard.[47] It would be inconsistent with the whole tenor of the hearings, especially the concerns expressed by CALEA co-sponsor Sen. Leahy, to conclude that Congress responded to these concerns by mandating an increase in the richness and accessibility of the signaling channel.

---

[46] *Id.* at 115.

[47] Jerry Berman of the Electronic Frontier Foundation raised the problem at the first CALEA hearing. *Id.* at 65.

(b) No significance can be attached to Congress' replacement of "call set-up information" with "call-identifying information"

The FBI has tried to pin its theory for an expansive reading of the call-identifying requirement on the fact that Congress used the term "call-identifying information" when it enacted CALEA, instead of the term "call set-up information," which had appeared in the draft transmitted to Congress by the Clinton Administration in March 1994. There is no evidence, however, suggesting that the reason for the change was to broaden the reach of the legislation, or that Congress viewed the term "call-identifying information" as defined in the Act as any broader than the term "call set-up information." To the contrary, all of the evidence indicates that Congress saw no difference between the terms.

Congress' intent is manifest in the Report's use of language to describe "call-identifying information" that is virtually identical to (and if anything, somewhat narrower than) the language used by the FBI to describe "call set-up information" when it submitted proposed legislation using the latter term.[48] It is obvious that the Committee Report's description of "call-identifying information" was copied from the FBI's description of "call set-up information," indicating that Congress saw no significant difference between the two terms.

Second, FBI Director Freeh testified as if the new phrase had no significance. In March 1994, when the term "call set-up information" was being used, his prepared statement said that the purpose of the statute was to "ensure that the content of communications and call set-up

---

[48] *Compare* House Report at 21(quoted above) *with* Hearings at 277-78, the section-by-section analysis that accompanied the FBI's draft including the phrase "call set-up information." It is interesting to note that the Committees' section-by-section description of "call-identifying information" is also very similar to the definition of "call set-up information" used by the FBI in the "Law Enforcement Requirements" document. Hearings at 290.

information (dialing information) can be intercepted."[49] In August, after the legislation was introduced using the term "call-identifying information," Freeh testified the problem to be addressed by the legislation was "the needed access to all communications and dialing information."[50]

Finally, when one *defined* term supersedes another *defined* term, it is not necessary to speculate about whether the new term in isolation is broader than the discarded one. It is only necessary to look at the enacted definition, informed by any report language and the legislative history other than the change itself. As explained above, the totality of these references indicates that the meaning of "call-identifying information" as defined by Congress is not significantly broader than the meaning of "call set-up information."

(c) The words "origin," "direction," "destination" and "termination"

The words "origin, "direction," "destination" and "termination" further limit the definition of call-identifying information. The word "origin" is obvious enough: it is the number from which the call began. "Destination" is equally obvious: it is the number to which the call is being made.[51] Indeed, this is where the definition started out in the FBI's first legislative

---

[49] *Id.* at 27.

[50] *Id.* at 115.

[51] The section-by-section analysis prepared by the FBI in the fall of 1992 to accompany an earlier version of the digital telephony legislation stated:

> Similarly, certain speed dialing features that mask the telephone called by the target must be identified for criminal law enforcement investigations. The ability to consistently determine the destination of calls is critical to minimizing the monitoring of innocent calls.

Linking "destination" to the problem of speed dialing indicates that the FBI wanted the 7 or 10 digits that were "masked" by speed dialing, not cell site or other physical location information and not status messages.

proposal in 1994; termination and direction did not appear in the FBI's April 1994 draft.[52] The original proposal read:

> 'call set-up information' shall mean the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization, including information associated with any telecommunication system dialing or calling features or services.[53]

In the course of redrafting, the terms "direction" and "termination" were added. "Direction" was added to acknowledge the difficult call-identifying problem associated with call forwarding. If the surveillance target is making a call to a person with call forwarding, the target's home switch (from which law enforcement obtains its surveillance access) cannot tell where the call will end up (i.e., its "destination"). If a pen register is placed on the target's line, or at the central office switch servicing the target, the pen register will only capture the number dialed or signaled by the target. The call will go to the switch that services that number, but it may be "redirected" to another number, and then another and another. It would not be practical to require the target's home switch to know the final destination of a call. All that the home switch of the target (and each intermediate switch) could provide contemporaneously would be the "direction" of the call as it passed through: the identity of the next number to which it was redirected. On the other hand, if the target is receiving a call that has been forwarded through various other numbers, the target's home switch (the last switch handling the call) may not know the "origin" of the call; it may only know the direction it came from most immediately. Finally, if the one using call forwarding is the surveillance target, the target's home switch will know

---

[52] Hearings at 267-68.

where the call has been redirected to, which may be the final destination point or may be yet another point from which it is forwarded. To reflect these various permutations of call redirection, Congress used the word "direction," since sometimes "direction" is all that is available to a carrier.

Finally, "termination" refers to the fact that a call (or call attempt) has ended by the surveillance target hanging up. That is, it refers to the duration of a call or call attempt. This information is obtained by a dialed number recorder (DNR), which is similar to a pen register, but also records the duration of calls by marking the time a phone went off-hook and the time it went back on-hook.[54] "Termination" thus means the time when a call ended, not how it ended. While there is little reference in the legislative history to "termination," and no reference could be found to dialed number recorders, the ending of a call by hanging up (off-hook, on-hook readings) is the meaning of the word most consistent with general law enforcement practice, as Congress understood it, especially in light of Congress' injunction that the requirements be interpreted narrowly.[55]

2. Regardless of the Meaning Attributed to Call-Identifying Information, Carriers are Only Required to Provide Data that is "Reasonably Available"

Congress was concerned that the "call-identifying" requirement would impose a burden on carriers, or that it would serve as the vehicle for law enforcement to expand the information

---

[53] *Id.*

[54] Although similar in function to the pen register, a DNR has the additional feature of recording the duration of all calls on the target phone, whether incoming or outgoing.

[55] The legislative history contains one reference in FBI Director Freeh's prepared testimony to "information generated by a caller which identifies the origin, duration, and destination" of a communication. Hearings at 33. This language was being used to describe "call set-up information;" when "call-identifying information" was adopted, the word "termination" was added to make it clear that duration was also covered.

content acquired by pen registers. Therefore, Congress limited the call-identifying requirement in a way it did not limit the call content requirement. The section of CALEA that establishes the call-identifying requirement requires carriers only to ensure that their systems are capable of isolating and intercepting call-identifying information "that is reasonably available." This means that even if a data element otherwise falls within the definition of "call-identifying information," carriers are not required to incorporate the capability to provide it to law enforcement unless it is reasonably available.

This is an important limitation on any interpretation of the call-identifying requirement. Certainly, Congress' inclusion of the phrase makes it very difficult for the FBI to contend that CALEA requires carriers to modify their systems to provide government access to signaling information that is not otherwise reasonably available on a contemporaneous basis. Indeed, the report of the Committees explicitly states, "However, if such [call-identifying] information is not reasonably available, the carrier does not have to modify its system to make it available."[56]

B. Location Information Does Not Fit within the Definition of Call-Identifying Information and Therefore Cannot Be Included in the Standard; Moreover, the FBI Specifically Testified that Location Information Was Excluded from CALEA

The interim industry standard requires cellular and PCS carriers to provide law enforcement agencies with location (cell site) information at the beginning and end of any cellular and PCS communication. Cell site or other location information cannot be found in any of the terms of the call-identifying information requirement. Location simply does not fit within the phrase "dialing or signaling information that identifies the origin, direction, destination, or

[56] House Report at p. 22.

termination of each communication." Clearly, "location" is not included in this list, and Congress could easily have included it. Each of the four terms in the list has a meaning related to the directory number of the calling or called party or the duration of the call, such that none of them can be stretched to also cover geographical location. Moreover, the location information sought by the FBI identifies the location of the telephone instrument, not the location of a "communication," which is what the Act refers to.[57]

Not only does location information not fit within the definition of call-identifying information, but it was the express intent of Congress, supported by the Director of the FBI on the record in public testimony, that CALEA not include any requirement to provide location or tracking information.

1. FBI Testimony Disavowed any Reading of the Statute which would Mandate Location Information as Part of the Call-Identifying Requirement

The concern that CALEA would mandate the availability of location information was a major source of privacy objections to the legislation in 1994. At the joint House and Senate hearings on March 18, 1994, FBI Director Freeh expressly testified that "call set-up information" (later changed to "call-identifying information") as a CALEA requirement was not intended to include location information. Director Freeh was very clear in disavowing any interest in covering such information:

> [Call set-up information] does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference

[57] The difficulty of fitting location information into the statutory definition is highlighted by a scenario in which both ends of a communication are mobile: what is the location of a "communication" when both the calling and the called parties are mobile.

> to this term, to acquire anything that could properly be called 'tracking' information.[58]

The legislative history contains nothing from the FBI or any other party to suggest an intent to reverse this position. There is nothing in the record to indicate that the FBI ever said that it was seeking the ability to acquire location information. It never listed inability to acquire location information as one of the problems that needed to be addressed.[59]

Eliminating location information as a CALEA mandate, however, did not solve the question of what to do with the fact that location information was nonetheless already available in some wireless systems and would be available in the future for reasons having nothing to do with CALEA.[60] Privacy advocates expressed concern that this information would be available with a mere pen register.[61] In response, Congress adopted a provision making it clear that if location information is available, it cannot be obtained by the government under a pen register or trap and trace order. (Congress did not specify what standard should be applied.) This provision started out as part of the definition of "call set-up information." When the term "call-identifying information" was adopted, the prohibition against providing location information as part of call-identifying information was moved out of the definition section and into the requirement section for call-identifying information.

---

[58] Hearings at 29, 33.

[59] House Report at 15.

[60] Director Freeh stated in his testimony, "[s]ome cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes." Hearings at 33. The Committee remained mindful of this; the Judiciary Committee report notes, "[c]urrently, in some cellular systems, transactional data that could be obtained by a pen register may include location information." House Report at 17.

[61] Hearings at 161.

After these changes were made, the FBI Director testified in support of the revised legislation, noting its reasonableness and its privacy protections. He never suggested in his testimony or in any other materials submitted for the record that any of the changes was intended to make location information -- one of the most contentious issues in the first hearing -- a CALEA mandate. By the time Freeh testified at the final CALEA hearings in August 1994, he appeared to accept the interpretation of Jerry Berman of the Electronic Frontier Foundation, who said that "[i]t is also important that one of the requirements that the committee has imposed is a requirement not to design ongoing location features into the electronic technology for communications. We do not want to turn our cellular and radio-based communication systems into nationwide tracking systems for persons who may be of interest to law enforcement and who are not subject to a warrant."[62] There was never any suggestion in the record that the assurance given by FBI Director Freeh on March 18 had been abandoned or that Congress intended to make location information a CALEA requirement.

2. The FBI Cannot Now Convert the Explicit Statutory Prohibition Against Providing Location Information Under Pen Register Orders into an Implied Requirement that Location be Provided under a Higher Standard

Since the enactment of CALEA, the FBI has claimed that the prohibition against providing location information under the minimal standard for a pen register or trap and trace device is actually a mandate for location information. The FBI now interprets this prohibition against providing location information in some cases as implying a requirement that location information must be uniformly available in other cases. But the statute does not state when or

---

[62] *Id.* at 158.

under what legal standard location information must be made available. An express prohibition against providing location information in some cases cannot be turned into an implied requirement to provide it in other, unspecified cases, especially given the FBI's express and never retracted assurances on the record that location information was not mandated by CALEA and Congress' injunction that the CALEA requirements must be narrowly interpreted.

The industry's decision to yield to the FBI and add location information to the J-STD violated Congress' intent that the capability assistance requirements of CALEA would serve as "both a floor and a ceiling" for government surveillance capabilities.[63] This statement by the Committees goes to the core of the balanced approach Congress intended in CALEA. The statute was intended to create a process for preserving a narrowly focused surveillance capability. It was not intended to afford the FBI leverage to steadily increase its capabilities. Changes in technology will bring ebbs and flows in government surveillance capability. The statute was not intended as a ratchet device to standardize every increase in the surveillance potential of telecommunications technology. By adding location information, carriers standardized a capability that Congress had specifically intended to exclude, violating Congress' ceiling principle.

CDT is not asking the Commission in this proceeding to require carriers to design their systems so they *cannot* provide location information. Under 18 U.S.C. § 2518(4), location information, if otherwise available, can be obtained under appropriate legal authority (but not under a pen register or trap and trace). But location information is not a CALEA mandate. Location information must be deleted from the CALEA safe harbor, because it goes beyond

---

[63] House Report at 22.

Congress' intended minimum, as reflected in Section103(a)(1) - (4). As far as CALEA is concerned, carriers should be free in the future, as they have been in the past, to build or not to build systems that generate and collect location information. Keeping it in the standard makes it a minimum requirement, contrary to the FBI's explicit assurances during the hearings, and contrary to Congress' intent that the capability requirements serve as a ceiling.

C. The Interim Industry Standard Fails to Protect Privacy in Packet Networks

Telecommunications systems rely increasingly on packet mode data transmission protocols such as those used on the Internet. In a packet network, communications are broken up into individual packets, each of which contains addressing information that helps route the packets to their intended destination, where they are reassembled. Currently utilized primarily on the Internet for data communications, this technology also offers substantial advantages in the voice environment as well, and telecommunications companies are beginning to incorporate it in their systems.

On the apparently untested assumption that it is not feasible to provide signaling information separate from content in a packet switching environment, industry's interim standard (Section 4.5.2) allows companies to deliver the entire packet data stream -- including the content of communications -- when law enforcement is entitled to receive only dialing or signaling information under a pen register order. The proposed CALEA standard relies on the law enforcement officials that conduct the interception to sort out the addressing information from the content, keeping the former but ignoring the latter.

Delivery of both signaling and content where only content is authorized to be intercepted violates Section 103(a)(4)(A) of CALEA, which requires carriers to ensure that their systems "protect[]the privacy and security of communications and call-identifying data not authorized to

be intercepted." The Commission should therefore delete Section 4.5.2 from the standard it ultimately establishes and issue guidance indicating how carriers and equipment manufacturers can comply with the CALEA requirement when implementing packet network services.

1. Section 4.5.2 of the Interim Standard Provides for the Delivery of Signaling Information Together With Message Content Even Where Only Signaling Information is Authorized to be Intercepted In Violation of Section 104(a)(4)(A) of CALEA

Section 4.5.2 of the standard allows packet data to be delivered to law enforcement by carriers in the same manner regardless of whether the law enforcement agency is authorized to receive signaling alone or both signaling and content. Under the terms of the standard, the carrier is allowed to provide the entire packet stream regardless of whether a law enforcement is entitled to receive content at all. The language of the standard currently provides:

> Packets shall be sent to the Collection Function when they are intercepted. The intercepted packets shall be delivered without interpretation or modification, expect for possible re-framing, segmentation, or enveloping required to transport the information to the Collection Function or except to remove information that is not authorized.

As we understand this provision, separation of signaling from content is allowed, but not required. CDT highlighted the inherent violation of Section 104 of CALEA in its ballot comments on the proposed industry standard. The draft was modified but it still falls short of requiring carriers to separate content from addressing. Instead, it relies on the government to sort out the addressing information from the content. This permissive approach to CALEA compliance, were it followed, could totally obliterate the distinction between call content and call-identifying information that was a core assumption of the Electronic Communications Privacy Act and of CALEA itself.

In the old analog telephone systems, law enforcement agencies authorized to receive dialing information were provided with access to the target's entire line, including content. With subsequent developments in technology, dialing information for call-routing purposes was carried on a channel separate from the call content. In this respect, technology itself can enhance privacy, creating an environment in which a law enforcement agency conducting a pen register would receive only so much as it was entitled to receive, and no more. Absent CALEA, packet networks might have undone that privacy enhancement, for both addressing and content travel together in packet-data systems. But through CALEA, Congress imposed on the telecommunications industry an affirmative obligation to protect communications not authorized to be intercepted. CALEA, Section 103(a)(4).

In a packet network environment, this means that carriers must separate addressing information from content (subject to CALEA's overall reasonably achievable standard).[64] The interim industry standard has failed to implement this requirement.

2. Compliance with Privacy Requirements Calling For Separation of Signaling and Message Content Information Appears Reasonably Achievable in at least some of the Packet Networks Discussed in Section 4.5.2

The standard mentions eight different packet network architectures and purports to be a safe harbor for all of these technologies. Generally available network analysis tools and

[64] We recognize that there are substantial open questions about the application of traditional pen register authority to new packet data networks, but the Commission need not resolve that question here. It is clear that the pen register statute could not, no matter what the technological context, grant law enforcement access to message content. So, though it may not be clear what information law enforcement is able to access under pen register authority, it is certainly clear that content is not included. Therefore the Section 104 requirement to protect the privacy of content during access to signaling alone applies.

techniques suggest that it is possible to separate signaling or addressing information from call content in at least some of the major packet network technologies covered by the standard.

X.25 networks, which are connection-oriented, contain separate and distinct call set-up and teardown messages. In this case, the carrier ought to be required to send law enforcement only the call set-up and teardown messages unless a full content interception is obtained. In another important network technology, TCP/IP (Internet) networks, packet headers are always of a fixed length and can therefore be automatically separated from the remaining portion of the packet. In this case, the carrier would send law enforcement the 20-byte IP headers after deleting everything that follows. Existing tools for network performance monitoring generally allow network technicians to copy from a data stream a specific number of bytes of each packet that contain just the protocol headers of interest. Similar network monitoring tools exist for Asynchronous Transfer Mode (ATM) networks as well as others mentioned in Section 4.5.2. Use of these tools would not only minimize the potential privacy invasion, but it would also greatly reduce the volume of data collected. Given that it is clearly reasonably achievable to meet the Section 104 privacy requirement in a number of the major packet networks covered by the standard, this section of the standard fails to meet statutory privacy protection requirements that are part of CALEA.

3. The Commission Should Replace the Current Provisions of Section 4.5.2 With a Requirement that Carriers Must Separate Signaling Information From Message Content

Having demonstrated that Section 4.5.2 of the current standard fails to meet the privacy requirements of CALEA Section 103, we believe that the Commission must strike this portion of the standard pursuant to CALEA Section 107. In its place, the Commission ought to rule that Section 103 requires carriers to deploy assistance capabilities along with packet technology in a

manner that enables them to separate packet addressing information from message content when responding to court orders authorizing only the deliver of addressing, but not content. Based on this finding, standards-bodies with expertise in the variety of packet network technologies being deployed today can then issue more precise guidance to their members, as they deem appropriate.

D. None of the Punch-List Items Are Required by CALEA

1. CALEA Does Not Require Carriers to Intercept the Communications of Those Who were Once Parties to a Conference Call with the Target of the Court Order; Rather, the Act Requires Carriers to Be Able to Intercept the New Call that the Targeted Individual Takes When He Drops off the Conference Call

The FBI claims that CALEA requires carriers to intercept the ongoing communications of parties on a conference call after the target of the investigation has dropped off the call and gone on to another call. At the time CALEA was enacted, the FBI expressed concern that three-way calling features interfered with its ability to listen to the communications of a target. Now, however, based on an overly-expansive reading of both the electronic surveillance laws and CALEA, the FBI would require carriers to build the capability to monitor all parties to a multi-party call even after the subject of the intercept order is no longer participating in the call. The purpose of CALEA was to follow the target, not to facilitate monitoring of those left behind after the subject of the court order is no longer on the call.

The first thing to note about this punch list item is that the DOJ/FBI plainly admit that this is not a status quo capability. Contrary to all the statements of the FBI at the Congressional hearings that CALEA was intended to preserve the wiretapping technique as it had existed since 1968, and contrary to the clear intent of the Committees that CALEA was intended to maintain

the status quo, the FBI admits in its petition that it wants this Commission to interpret CALEA to mandate a capability that has not been traditionally available to law enforcement.[65]

Nor is this punch list item required by the language of the Act. CALEA requires carriers to provide law enforcement with all wire and electronic communications "carried by the carrier to or from equipment, facilities or services of a subscriber." A conference call to which the subscriber is no longer a party is not a communication "carried by the carrier to or from the equipment, facilities or services of the subscriber." Recognizing this, the FBI would change the reading of the Act to "all wire and electronic communications *supported by a subscriber's service.*"[66] This is clearly a broader reading than the words of the statute will sustain. A conference call that the subscriber has dropped off of may still be "supported" by the subscriber's service in some theoretical way, but it is not carried to or from the equipment, facilities or services of the subscriber.

Moreover, the words "equipment, facilities, or services" must be read carefully. "Equipment" is clear enough; it has a physical connotation, referring to a wireless phone, for example. "Facilities" is drawn from Title III. It was adopted in 1968, long before there were wireless phones; it too has a physical connotation. Only the word "services" could possibly support the FBI's conference calling proposal, and it seems that Congress used the term to refer to instances where a targeted subscriber might evade interception of communications to which he or she was a party. It was in this context that FBI Director Freeh in his testimony used the word "services" to refer to services that "undermine the necessity for communications to be

---

[65] *See* DOJ/FBI Petition at ¶ 51.

[66] *Id.* at ¶ 55.

transmitted always to the same specific location or through the same wireline loop."[67] The Director was referring to call forwarding or "follow-me-type" services, where the concern was that law enforcement would miss the communication of the subscriber to the service.

The Committees' report confirms this narrow reading, specifically stating that CALEA would require carriers "to ensure that new technologies and services do not hinder law enforcement access to *the communications of a subscriber who is the subject of a court order.*"[68] A conference call to which the subscriber is no longer a party is not a "communication of the subscriber who is the subject of the court order." It is a communication of two or more other people.

In explaining the justification for the three way calling requirement, the DOJ/FBI now posit the following hypothetical:

> Under the interim standard, an intercept subject might initiate a conference call with two associates, A and B, then place A and B on hold while answering an incoming call. A and B could continue talking while the subject speaks to the incoming caller on another line. Law enforcement would not receive the content of the conversation between A and B, even though that conversation is being supported by the subscriber's service or carried by the subscriber's facilities, may be legally intercepted under the Title III order, and is pertinent to the criminal activity under investigation.[69]

What the DOJ and the FBI fail to state is that the reason why law enforcement would not receive the conversation between A and B is because the carrier would be intercepting and providing to law enforcement the conversation that the intercept target was having with the new caller. The purpose of CALEA is to ensure that new technologies like call conferencing do not

---

[67] Hearings at 24.

[68] House Report at 16 (emphasis added.)

interfere with the interception of calls to the intercept target. Law enforcement would have something to complain about if carriers said that once having established an interception on the conference call, they could not create a new interception on the new call that the intercept target accepts. But that is not what carriers are proposing. They have agreed to provide the capability to intercept the new conversation.

We doubt that the particularity requirement of the Fourth Amendment, reflected in Title III's Section 2518, would support a court order for the communications of presumptively innocent third parties when the targeted party is no longer on the call. As the DOJ/FBI acknowledge, an interception is directed either at a particular person or at particular facilities. Law enforcement may intercept either the named person or anybody using a named facility. It may not intercept an unnamed party using an unnamed facility.

2. CALEA does not Require the Carrier Originating a Call to Provide Post-Cut through Dialed Digits; the FBI Specifically Assured Congress that this was not Covered by CALEA's Call-Identifying Information Requirement

When a person uses a long distance calling card, he or she first dials the 800 or local number that leads to the long distance carrier's system. The local carrier, if served with a pen register order, would be required to intercept the seven digit or 800 access number, but the carrier would then establish a content channel for the calling party and treat the call as connected from its perspective. Then the caller may be prompted by the long distance carrier to dial additional numbers, including the desired ultimate destination of the long-distance toll call. To the system

---

[69] FBI/DOJ Petition at ¶ 52.

of the local exchange carrier complying with a surveillance order, these digits dialed after call cut-through do not identify a call. By definition, they are "post cut-through." This means that, for the carrier complying with the order, the call has been properly routed and any further dialed digits are treated as indistinguishable from other content. Law enforcement wishing to intercept these post cut-through digits has two choices: serve the first carrier with a content interception order, or serve the long-distance carrier, which does treat the digits as call-routing information, with a pen register order or subpoena. The FBI does not want to make this choice. It wants to interpret CALEA to require the first carrier to provide the post cut-through digits under the much weaker pen register standard.

The issue here, contrary to the claim of DOJ/FBI in their Petition at ¶ 71, is not the loss of post cut-through dialed digits. Law enforcement will still be able to determine the destination of subject-initiated calls. That information is of course available to law enforcement on the content channel with Title III authorization or from the target's long distance carrier with a mere pen register order or subpoena. The issue is whether the FBI can use CALEA to reduce the standard for access to information that carriers treat as content and avoid going to the long distance carrier.

Congress made it clear that CALEA was "not intended to guarantee 'one-stop shopping' for law enforcement."[70] Yet that is precisely what the government wants here.

The legislative history makes it clear that "call-identifying information" does not include dialed numbers after call cut-through. In his initial testimony on CALEA, FBI Director Freeh derided some CALEA critics for raising what Freeh called the "false 'transactional data scare.'"

---

[70] House Report at 22.

Freeh was very explicit in saying that CALEA was intended to cover only the "dialing information derived from a pen register," as distinguished from the transactional data. Freeh's testimony specifically addressed the situation involving long distance credit card calls:

> The dialing information derived from a pen register is obtained by law enforcement and is limited to a *specific telephone line and number*. On the other hand, transactional billing information is compiled . . . from *every telephone a subscriber may use* during the billing period, such as credit card calls . . . .[71]

There is another reason why post cut-through dialed digits are not covered: a local carrier will have no way to tell which post-cut through dialed digits are for call-processing purposes and which are content. There are times when post-cut through dialed digits are clearly not call-identifying information. For example, when a person calls her bank-by -phone number and uses an automatic prompt system and the dial pad to access various bank services, those dialed digits are not call-identifying in any way. They are clearly content. On the other hand, when a person using a long-distance calling card calls a local or 800 access number, some of the digits dialed after the prompt are used for call-processing while others are for phone company billing purposes and are not call-identifying information under any reading of the definition.

To do what the FBI asks, the local carrier will inevitably provide content to law enforcement under the lower pen register standard, which is precisely what Congress wanted to avoid. Contrary to the FBI's assertion in its Petition, there is a privacy based constraint that prevents carriers from providing content in response to a pen register.

Finally, even if the post-cut through digits were considered to be call-identifying information, they are mixed in with content and therefore are not "reasonably available" to the

---

[71] Hearings at 32 (emphasis in original).

local carrier on a signaling channel. Section 103(a)(2) only requires carriers to provide "reasonably available" call-identifying information.

3. The Detailed Signaling Data Sought by the FBI Does Not Fit the Definition of Call-Identifying Information.

FBI Director Freeh repeatedly assured the Congress that call-identifying information was limited to dialed number information. "What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I now have under pen register authority."[72]

In their petition, the DOJ and the FBI now contend that the requirement to provide call-identifying information encompasses a truly dazzling array of signaling information. It is difficult to parse from their Petititon all the specific items of information that the FBI believes are encompassed by the phrase "call-identifying information," but they would include the following (all citations are to the DOJ/FBI petition):[73]

(1) Flash hook messages (¶¶ 58, 61):[74] The FBI claims (¶ 63) that this is necessary "to follow the course of the conversation [and] determine to whom the subject is speaking at any point in the conversation." For this punch list item, as for many of others, the FBI has developed a totally new justification. No longer is the FBI interested in identifying the origin, destination, direction or termination of the call. Instead, the FBI wants (¶ 59) this capability so that it can "identify the parties to the call." This is the exact opposite of the common understanding of the

---

[72] *Id.* at 50.

[73] This list shows that the FBI's "punch list" is not limited to eleven items, as the FBI claimed last year, or nine, but is a list of items within items, each of which can be expanded at the FBI's whim, making it impossible for carriers or subscribers to ever know with certainty what surveillance capabilities are required of the American phone system.

[74] *See also* DOJ/FBI Petition at ¶¶58, 61 (transfer key message).